PCT/JP2004/015752

18.10.2004

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年１０月１６日

出願番号
Application Number: 特願２００３－３５６０７３

[ST. 10/C]: [ＪＰ２００３－３５６０７３]

出願人
Applicant(s): 松下電器産業株式会社

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

２００４年１１月１８日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

出証番号　出証特２００４－３１０４７４

【書類名】　特許願
【整理番号】　2022550348
【提出日】　平成15年10月16日
【あて先】　特許庁長官殿
【国際特許分類】　G09C　5/00
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　布田　裕一
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　山道　将人
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　大森　基司
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　館林　誠
【特許出願人】
　【識別番号】　000005821
　【氏名又は名称】　松下電器産業株式会社
【代理人】
　【識別番号】　100097445
　【弁理士】
　【氏名又は名称】　岩橋　文雄
【選任した代理人】
　【識別番号】　100103355
　【弁理士】
　【氏名又は名称】　坂口　智康
【選任した代理人】
　【識別番号】　100109667
　【弁理士】
　【氏名又は名称】　内藤　浩樹
【手数料の表示】
　【予納台帳番号】　011305
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9809938

【書類名】特許請求の範囲
【請求項１】
第１の機器と第２の機器を備え、前記第１の機器と前記第２の機器との間で鍵配送を行い、共有した鍵を用いて前記第１の機器から前記第２の機器へコンテンツデータを送信する暗号通信システムであって、
前記第１の機器は、
第１の公開鍵証明書と第１のコンテンツデータを格納する第１のデータ格納部と、
前記第２の機器へデータを送信する第１の送信部と、
前記第２の機器から送信されたデータを受信する第１の受信部と、
第２の公開鍵証明書を検証する第１の証明書検証部と、
第１の鍵と第１の鍵を暗号化した第１の暗号化鍵を生成する第１の暗号化鍵生成部と、
第２の暗号化鍵から復号化し、復号化した結果を第２の鍵として出力する第１の暗号化鍵復号部と、
前記第１の鍵と前記第２の鍵に基づき共有鍵を生成する共有鍵生成部と、
前記共有鍵を格納する共有鍵格納部と、
前記共有鍵の一部または全部を用いて、前記第１のコンテンツデータを共通鍵暗号を用いて暗号化した第１の暗号化コンテンツデータと、前記共有鍵の一部または全部と鍵付ハッシュ関数を用いて第１のハッシュ値を生成する第１の暗号化部とを含み、
前記第２の機器は、
前記第２の公開鍵証明書と前記第２のコンテンツデータを格納する第２のデータ格納部と、
前記第１の機器へデータを送信する第２の送信部と、
前記第１の機器から送信されたデータを受信する第２の受信部と、
前記第１の公開鍵証明書を検証する第２の証明書検証部と、
第２の鍵と第２の鍵を暗号化した前記第２の暗号化鍵を生成する第２の暗号化鍵生成部と、
前記第１の暗号化鍵から復号化し、復号化した結果を前記第１の鍵として出力する第２の暗号化鍵復号部と、
前記第１の鍵と前記第２の鍵に基づき共有鍵を生成する前記共有鍵生成部と、
前記共有鍵を格納する前記共有鍵格納部と、
前記第１の暗号化コンテンツデータを復号化し、第１の復号コンテンツデータを取得し、前記第１の復号コンテンツデータに対して、前記共有鍵の一部または全部と前記鍵付ハッシュ関数を用いて第２のハッシュ値を生成し、前記第１のハッシュ値と比較する第１の復号化部とを含むこと
を特徴とする暗号通信システム。
【請求項２】
第１の機器はさらに、第２の暗号化コンテンツデータを復号化し、第２の復号コンテンツデータを取得し、前記第２の復号コンテンツデータに対して、前記共有鍵の一部または全部と前記鍵付ハッシュ関数を用いて第３のハッシュ値を生成し、第４のハッシュ値と比較する第２の復号化部を含み、
第２の機器はさらに、前記共有鍵の一部または全部を用いて、前記第２のコンテンツデータを暗号化した前記第２の暗号化コンテンツデータと、前記共有鍵の一部または全部と鍵付ハッシュ関数を用いて前記第４のハッシュ値を生成する第２の暗号化部を含むこと
を特徴とする請求項１記載の暗号通信システム。
【請求項３】
前記第１の暗号化鍵及び前記第２の暗号化鍵は、鍵カプセル化メカニズムを用いて生成すること
を特徴とする請求項１または請求項２記載の暗号通信システム。
【請求項４】
前記共有鍵生成部は、前記第１の鍵と前記第２の鍵の排他的論理和を前記共有鍵として出

力すること
を特徴とする請求項１から請求項３のいずれか１項に記載の暗号通信システム。
【請求項５】
前記共有鍵生成部は、前記第１の鍵と前記第２の鍵をビット連結したものをハッシュ関数を用いて計算したハッシュ値を前記共有鍵として出力すること
を特徴とする請求項１から請求項３のいずれか１項に記載の暗号通信システム。
【請求項６】
第１の機器と第２の機器を備え、前記第１の機器と前記第２の機器との間で鍵配送を行う認証鍵共有システムであって、
前記第１の機器は、
第１の公開鍵証明書と第１のコンテンツデータを格納する第１のデータ格納部と、
前記第２の機器へデータを送信する第１の送信部と、
前記第２の機器から送信されたデータを受信する第１の受信部と、
第２の公開鍵証明書を検証する第１の証明書検証部と、
鍵カプセル化メカニズムを用いて第１の鍵と第１の鍵を暗号化した第１の暗号化鍵を生成する第１の暗号化鍵生成部と、
第２の暗号化鍵から復号化し、第２の鍵を出力する第１の暗号化鍵復号部と、
前記第１の鍵と前記第２の鍵に基づき共有鍵を生成する共有鍵生成部と、
前記共有鍵を格納する共有鍵格納部とを含み、
前記第２の機器は、
前記第２の公開鍵証明書と前記第２のコンテンツデータを格納する第２のデータ格納部と、
前記第１の機器へデータを送信する第２の送信部と、
前記第１の機器から送信されたデータを受信する第２の受信部と、
前記第１の公開鍵証明書を検証する第２の証明書検証部と、
第２の鍵と第２の鍵を暗号化した前記第２の暗号化鍵を生成する第２の暗号化鍵生成部と、
前記第１の暗号化鍵から復号化し、前記第１の鍵を出力する第２の暗号化鍵復号部と、
前記第１の鍵と前記第２の鍵に基づき共有鍵を生成する前記共有鍵生成部と、
前記共有鍵を格納する前記共有鍵格納部とを含むこと
を特徴とする認証鍵共有システム。
【請求項７】
コンテンツ送信機器とコンテンツ受信機器を備え、前記コンテンツ送信機器と前記コンテンツ受信機器との間で鍵配送を行い、共有した鍵を用いて暗号化通信を行う暗号通信システムにおけるコンテンツ送信機器であって、
第１の公開鍵証明書と第１のコンテンツデータを格納する第１のデータ格納部と、
前記コンテンツ受信機器へデータを送信する第１の送信部と、
前記コンテンツ受信機器から送信されたデータを受信する第１の受信部と、
前記コンテンツ受信機器に対する第２の公開鍵証明書を検証する第１の証明書検証部と、
第１の鍵と第１の鍵を暗号化した第１の暗号化鍵を生成する第１の暗号化鍵生成部と、
前記コンテンツ受信機器から送信される第２の暗号化鍵を復号化し、復号化した結果を第２の鍵として出力する第１の暗号化鍵復号部と、
前記第１の鍵と前記第２の鍵に基づき共有鍵を生成する共有鍵生成部と、
前記共有鍵を格納する共有鍵格納部と、
前記共有鍵の一部または全部を用いて、前記第１のコンテンツデータを共通鍵暗号を用いて暗号化した第１の暗号化コンテンツデータと、前記共有鍵の一部または全部と鍵付ハッシュ関数を用いて第１のハッシュ値を生成する第１の暗号化部とを備えること
を特徴とするコンテンツ送信機器。
【請求項８】

前記第１の暗号化鍵は、鍵カプセル化メカニズムを用いて生成すること
を特徴とする請求項７記載のコンテンツ送信機器。
【請求項９】
前記共有鍵生成部は、前記第１の鍵と前記第２の鍵の排他的論理和を前記共有鍵として出力すること
を特徴とする請求項７または請求項８記載のコンテンツ送信機器。
【請求項１０】
前記共有鍵生成部は、前記第１の鍵と前記第２の鍵をビット連結したものをハッシュ関数を用いて計算したハッシュ値を前記共有鍵として出力すること
を特徴とする請求項７または請求項８記載のコンテンツ送信機器。
【請求項１１】
コンテンツ送信機器とコンテンツ受信機器を備え、前記コンテンツ送信機器と前記コンテンツ受信機器との間で鍵配送を行い、共有した鍵を用いて暗号化通信を行う暗号通信システムにおけるコンテンツ受信機器であって、
第２の公開鍵証明書と第２のコンテンツデータを格納する第２のデータ格納部と、
前記コンテンツ送信機器へデータを送信する第２の送信部と、
前記コンテンツ送信機器から送信されたデータを受信する第２の受信部と、
前記コンテンツ送信機器に対する第１の公開鍵証明書を検証する第２の証明書検証部と、
第２の鍵と第２の鍵を暗号化した第２の暗号化鍵を生成する第２の暗号化鍵生成部と、
前記コンテンツ送信機器から送信された第１の暗号化鍵を復号化し、復号化した結果を第１の鍵として出力する第２の暗号化鍵復号部と、
前記第１の鍵と第２の鍵に基づき共有鍵を生成する共有鍵生成部と、
前記共有鍵を格納する共有鍵格納部と、
前記コンテンツ送信機器から送信された第１の暗号化コンテンツデータを復号化し、第１の復号コンテンツデータを取得し、前記第１の復号コンテンツデータに対して、前記共有鍵の一部または全部と鍵付ハッシュ関数を用いて第２のハッシュ値を生成し、第１のハッシュ値と比較する第１の復号化部とを備えること
を特徴とするコンテンツ受信機器。
【請求項１２】
前記第２の暗号化鍵は、鍵カプセル化メカニズムを用いて生成すること
を特徴とする請求項１１記載のコンテンツ受信機器。
【請求項１３】
前記共有鍵生成部は、前記第１の鍵と前記第２の鍵の排他的論理和を前記共有鍵として出力すること
を特徴とする請求項１１または請求項１２記載のコンテンツ受信機器。
【請求項１４】
前記共有鍵生成部は、前記第１の鍵と前記第２の鍵をビット連結したものをハッシュ関数を用いて計算したハッシュ値を前記共有鍵として出力すること
を特徴とする請求項１１または請求項１２記載のコンテンツ受信機器。
【請求項１５】
第１の機器と第２の機器を備え、前記第１の機器と前記第２の機器との間で鍵配送を行い、共有した鍵を用いて前記第１の機器から前記第２の機器へコンテンツデータを送信する暗号通信方法であって、
第１の公開鍵証明書と第１のコンテンツデータを格納する第１のデータ格納ステップと、
前記第２の機器へデータを送信する第１の送信ステップと、
前記第２の機器から送信されたデータを受信する第１の受信ステップと、
第２の公開鍵証明書を検証する第１の証明書検証ステップと、
第１の鍵と第１の鍵を暗号化した第１の暗号化鍵を生成する第１の暗号化鍵生成ステッ

プと、
　第２の暗号化鍵から復号化し、復号化した結果を第２の鍵として出力する第１の暗号化鍵復号ステップと、
　前記第１の鍵と前記第２の鍵に基づき共有鍵を生成する共有鍵生成ステップと、
　前記共有鍵を格納する共有鍵格納ステップと、
　前記共有鍵の一部または全部を用いて、前記第１のコンテンツデータを共通鍵暗号を用いて暗号化した第１の暗号化コンテンツデータと、前記共有鍵の一部または全部と鍵付ハッシュ関数を用いて第１のハッシュ値を生成する第１の暗号化ステップとを前記第１の機器に実行させ、
　前記第２の公開鍵証明書と前記第２のコンテンツデータを格納する第２のデータ格納ステップと、
　前記第１の機器へデータを送信する第２の送信ステップと、
　前記第１の機器から送信されたデータを受信する第２の受信ステップと、
　前記第１の公開鍵証明書を検証する第２の証明書検証ステップと、
　第２の鍵と第２の鍵を暗号化した前記第２の暗号化鍵を生成する第２の暗号化鍵生成ステップと、
　前記第１の暗号化鍵から復号化し、復号化した結果を前記第１の鍵として出力する第２の暗号化鍵復号ステップと、
　前記第１の鍵と前記第２の鍵に基づき共有鍵を生成する前記共有鍵生成ステップと、
　前記共有鍵を格納する前記共有鍵格納ステップと、
　前記第１の暗号化コンテンツデータを復号化し、第１の復号コンテンツデータを取得し、前記第１の復号コンテンツデータに対して、前記共有鍵の一部または全部と前記鍵付ハッシュ関数を用いて第２のハッシュ値を生成し、前記第１のハッシュ値と比較する第１の復号化ステップとを前記第２の機器に実行させること
　を特徴とする暗号通信方法。
【請求項１６】
第１の機器はさらに、第２の暗号化コンテンツデータを復号化し、第２の復号コンテンツデータを取得し、前記第２の復号コンテンツデータに対して、前記共有鍵の一部または全部と前記鍵付ハッシュ関数を用いて第３のハッシュ値を生成し、第４のハッシュ値と比較する第２の復号化ステップを含み、
　第２の機器はさらに、前記共有鍵の一部または全部を用いて、前記第２のコンテンツデータを暗号化した前記第２の暗号化コンテンツデータと、前記共有鍵の一部または全部と鍵付ハッシュ関数を用いて前記第４のハッシュ値を生成する第２の暗号化ステップを含むこと
　を特徴とする請求項１５記載の暗号通信方法。
【請求項１７】
前記第１の暗号化鍵及び前記第２の暗号化鍵は、鍵カプセル化メカニズムを用いて生成すること
　を特徴とする請求項１５または請求項１６記載の暗号通信方法。
【請求項１８】
コンテンツ送信機器とコンテンツ受信機器を備え、前記コンテンツ送信機器と前記コンテンツ受信機器との間で鍵配送を行い、共有した鍵を用いて暗号化通信を行う暗号通信システムにおけるコンテンツ送信機器で実行されるプログラムであって、
　第１の公開鍵証明書と第１のコンテンツデータを格納する第１のデータ格納ステップと、
　前記コンテンツ受信機器へデータを送信する第１の送信ステップと、
　前記コンテンツ受信機器から送信されたデータを受信する第１の受信ステップと、
　前記コンテンツ受信機器に対する第２の公開鍵証明書を検証する第１の証明書検証ステップと、
　第１の鍵と第１の鍵を暗号化した第１の暗号化鍵を生成する第１の暗号化鍵生成ステッ

プと、
　前記コンテンツ受信機器から送信される第２の暗号化鍵を復号化し、復号化した結果を第２の鍵として出力する第１の暗号化鍵復号ステップと、
　前記第１の鍵と前記第２の鍵に基づき共有鍵を生成する共有鍵生成ステップと、
　前記共有鍵を格納する共有鍵格納ステップと、
　前記共有鍵の一部または全部を用いて、前記第１のコンテンツデータを共通鍵暗号を用いて暗号化した第１の暗号化コンテンツデータと、前記共有鍵の一部または全部と鍵付ハッシュ関数を用いて第１のハッシュ値を生成する第１の暗号化ステップとをコンテンツ送信機器に実行させること
　を特徴とするプログラム。
【請求項１９】
コンテンツ送信機器とコンテンツ受信機器を備え、前記コンテンツ送信機器と前記コンテンツ受信機器との間で鍵配送を行い、共有した鍵を用いて暗号化通信を行う暗号通信システムにおけるコンテンツ受信機器で実行されるプログラムであって、
　第２の公開鍵証明書と第２のコンテンツデータを格納する第２のデータ格納ステップと、
　前記コンテンツ送信機器へデータを送信する第２の送信ステップと、
　前記コンテンツ送信機器から送信されたデータを受信する第２の受信ステップと、
　前記コンテンツ送信機器に対する前記第１の公開鍵証明書を検証する第２の証明書検証ステップと、
　第２の鍵と第２の鍵を暗号化した第２の暗号化鍵を生成する第２の暗号化鍵生成ステップと、
　前記コンテンツ送信機器から送信された第１の暗号化鍵を復号化し、復号化した結果を前記第１の鍵として出力する第２の暗号化鍵復号ステップと、
　前記第１の鍵と前記第２の鍵に基づき共有鍵を生成する共有鍵生成ステップと、
　前記共有鍵を格納する共有鍵格納ステップと、
　前記コンテンツ送信機器から送信された第１の暗号化コンテンツデータを復号化し、第１の復号コンテンツデータを取得し、前記第１の復号コンテンツデータに対して、前記共有鍵の一部または全部と前記鍵付ハッシュ関数を用いて第２のハッシュ値を生成し、前記第１のハッシュ値と比較する第１の復号化ステップとをコンテンツ受信機器に実行させること
　を特徴とするプログラム。
【請求項２０】
請求項１８または請求項１９に記載のプログラムを記録した媒体。

【書類名】明細書
【発明の名称】暗号通信システム、認証鍵共有システム、コンテンツ送信機器、コンテンツ受信機器及び暗号通信方法
【技術分野】
【０００１】
本発明は、情報セキュリティ技術としての暗号技術に関する。
【背景技術】
【０００２】
近年、家庭用電化製品、携帯電話などの間でネットワークを介した通信を行う機会が増加している。例えば、ＡＶ機器では、コンテンツの著作権保護のために、機器同士で、また、携帯電話では通信内容の漏洩を防ぐため、認証鍵共有を行った後に、共有した鍵を用いて暗号化した通信を行うことがある。ここで、認証鍵共有とは、機器同士などで、通信相手の機器が正しく作られた機器であるかを、相互認証により確認し、それと同時に鍵を共有するものである。以下は、ＡＶ機器同士をＩＥＥＥ１３９４で接続したときに使用される、ＤＴＣＰ（Ｄｉｇｉｔａｌ　Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｃｏｎｔｅｎｔ　Ｐｒｏｔｅｃｔｉｏｎ）と呼ばれる著作権保護規格で規定されている認証鍵共有方法を示している（非特許文献１参照）。この方法は、認証方式に楕円ＤＳＡ署名を用いたチャレンジ・レスポンス認証を使用し、鍵共有方式に楕円ＤＨ鍵共有を使用している。チャレンジ・レスポンス認証、楕円ＤＳＡ署名及び楕円ＤＨ鍵共有については、非特許文献２が詳しい。図４でその処理を示す。
【０００３】
（従来例１：認証鍵共有）
以下では従来例１である認証鍵共有方法の処理を示す。以下の認証鍵共有方法ではユーザＡとＢとの間で相互認証及び鍵共有を行う。なお、ユーザＡは公開鍵証明書Ｃｅｒｔ＿Ａとそれに対応する秘密鍵ＫＳＡ及びセンタ公開鍵ＫＰＣを保持する。ユーザＢは公開鍵証明書Ｃｅｒｔ＿Ｂとそれに対応する秘密鍵ＫＳＢ及びセンタ公開鍵ＫＰＣを保持する。
【０００４】
ステップＳ２０１：ユーザＢはまず、ユーザＡに自身の公開鍵証明書Ｃｅｒｔ＿Ｂとチャレンジデータｃ Ｂを送る。ここで、Ｃｅｒｔ＿Ｂは、Ｂの公開鍵ＫＰＢとそのセンタ署名ＳＣＢ＝Ｓｉｇ（ＫＳＣ，ＫＰＢ）である。ここで、Ｓｉｇ（ＫＳＣ，ＫＰＢ）はセンタ秘密鍵ＫＳＣを用いて作成した公開鍵ＫＰＢに対する署名データである。
【０００５】
ステップＳ２０２：次にユーザＡは、Ｃｅｒｔ＿Ｂ、ｃ Ｂを受信し、Ｃｅｒｔ＿Ｂに含まれる公開鍵ＫＰＢとその署名ＳＣＢに対して、センタ公開鍵ＫＰＣを用いて、署名ＳＣＢが公開鍵ＫＰＢに対する正しいセンタ署名であるかを検証する。その結果、正しいセンタ署名でなければ処理を終了させる。正しいセンタ署名であれば、次のステップＳ２０３へ進む。
【０００６】
ステップＳ２０３：ユーザＡは、自身の公開鍵証明書Ｃｅｒｔ＿Ａとチャレンジデータｃ Ａをユーザ Ｂに送信する。ここで、Ｃｅｒｔ＿Ａは、Ａの公開鍵ＫＰＡとそのセンタ署名ＳＣＡ＝Ｓｉｇ（ＫＳＣ，ＫＰＡ）である。
【０００７】
ステップＳ２０４：ユーザＢは、Ｃｅｒｔ＿Ａ、ｃ Ａを受信し、Ｃｅｒｔ＿Ａに含まれる公開鍵ＫＰＢとその署名ＳＣＡに対して、センタ公開鍵ＫＰＣを用いて、署名ＳＣＡが公開鍵ＫＰＢに対する正しいセンタ署名であるかを検証する。その結果、正しいセンタ署名でなければ処理を終了させる。正しいセンタ署名であれば、次のステップＳ２０５へ進む。
【０００８】
ステップＳ２０５：ユーザＡは、乱数ｋＡを発生させ、楕円ＤＨ鍵共有の第１フェーズの値ｋＡ＊Ｇを計算する。ここで、Ｇは、ベース点であり、ｋＡ＊Ｇは楕円曲線上の点Ｇ

をｋＡ回加算することにより得られる楕円曲線上の点を表す。

【０００９】

ステップＳ２０６：ユーザＡは、ｃＢとｋＡ＊Ｇの連結に対して、秘密鍵ＫＳＡを用いて、署名ＳＡ＝Ｓｉｇ（ＫＳＡ，ｃＢ｜｜ｋＡ＊Ｇ）を作成する。ここで、ｘ｜｜ｙはｘとｙの連結を示す。

【００１０】

ステップＳ２０７：ユーザＡは、ｃＢ、ｋＡ＊Ｇ及びＳＡをユーザＢに送信する。

【００１１】

ステップＳ２０８：ユーザＢは、ｃＢ、ｋＡ＊Ｇ及びＳＡを受信し、ユーザＡの公開鍵ＫＰＡを用いて、署名ＳＡがｃＢとｋＡ＊Ｇの連結に対する正しい署名であるか検証する。正しくなければ、システムを終了させる。それ以外は次のステップＳ２０９へ進む。

【００１２】

ステップＳ２０９：ユーザＢは、乱数ｋＢを発生させ、楕円ＤＨ鍵共有の第１フェーズの値ｋＢ＊Ｇを計算する。

【００１３】

ステップＳ２１０：ユーザＢは、ｃＡとｋＢ＊Ｇの連結に対して、秘密鍵ＫＳＢを用いて、署名ＳＢ＝Ｓｉｇ（ＫＳＢ，ｃＡ｜｜ｋＢ＊Ｇ）を作成する。

【００１４】

ステップＳ２１１：ユーザＢは、ｃＡ、ｋＢ＊Ｇ及びＳＢをユーザＡに送信する。

【００１５】

ステップＳ２１２：ユーザＡは、ｃＡ、ｋＢ＊Ｇ及びＳＢを受信し、ユーザＢの公開鍵ＫＰＢを用いて、署名ＳＢがｃＡとｋＢ＊Ｇの連結に対する正しい署名であるか検証する。正しくなければ、システムを終了させる。それ以外は次のステップＳ２１３へ進む。

【００１６】

ステップＳ２１３：ユーザＢは、ｋＡ＊ＧとｋＢを用いて、ｋＢ＊（ｋＡ＊Ｇ）を計算し、それを共有鍵とする。

【００１７】

ステップＳ２１４：ユーザＡは、ｋＢ＊ＧとｋＡを用いて、ｋＡ＊（ｋＢ＊Ｇ）を計算し、それを共有鍵とし、終了する。

【００１８】

また、最近、公開鍵暗号においては、数学的な問題が求解困難である場合に、秘密鍵を持たないユーザが暗号文を解読することができないという安全性の証明をすることが多くなってきている。この安全性の証明により、公開鍵暗号の安全性の保証をする。このような証明を「安全性証明」と呼ぶ。例えば、楕円曲線を利用するＥＣＩＥＳ暗号は、ａ＊Ｇとｂ＊Ｇから、ａ＊（ｂ＊Ｇ）を求めるＤｉｆｆｉｅ－Ｈｅｌｌｍａｎ問題と呼ばれる問題が求解困難である場合に、安全であることが証明されている。ＥＣＩＥＳ暗号及びその証明については、非特許文献６が詳しい。

【非特許文献１】ＤＴＣＰ　ＳｐｅｃｉｆｉｃａｔｉｏｎのＷｈｉｔｅ　ｐａｐｅｒ＜ＵＲＬ：ｈｔｔｐ：／／ｗｗｗ．ｄｔｃｐ．ｃｏｍ／ｓｐｅｃ．ｈｔｍｌ＞

【非特許文献２】岡本龍明、山本博資、”現代暗号”、産業図書（１９９７年）

【非特許文献３】Ｖｉｃｔｏｒ　Ｓｈｏｕｐ，“Ａ　ｐｒｏｐｏｓａｌ　ｆｏｒ　ａｎ　ＩＳＯ　ｓｔａｎｄａｒｄ　ｆｏｒ　ｐｕｂｌｉｃ　ｋｅｙ　ｅｎｃｒｙｐｔｉｏｎ　（ｖｅｒｓｉｏｎ　２．１）”、［ｏｎｌｉｎｅ］、２００１年１２月２０日、［２００２年９月２９日検索］、インターネット＜ＵＲＬ：　ｈｔｔｐ：／／ｓｈｏｕｐ．ｎｅｔ／ｐａｐｅｒｓ／ｉｓｏ－２＿１．ｐｄｆ＞

【非特許文献４】Ｔａｔｓｕａｋｉ　Ｏｋａｍｏｔｏ，“Ｇｅｎｅｒｉｃ　ｃｏｎｖｅｒｓｉｏｎｓ　ｆｏｒ　ｃｏｎｓｔｒｕｃｔｉｎｇ　ＩＮＤ－ＣＣＡ２　ｐｕｂｌｉｃ－ｋｅｙ　ｅｎｃｒｙｐｔｉｏｎ　ｉｎ　ｔｈｅ　ｒａｎｄｏｍ　ｏｒａｃｌｅ　ｍｏｄｅｌ”、［ｏｎｌｉｎｅ］、Ｔｈｅ　５ｔｈ　Ｗｏｒｋｓｈｏｐ　ｏｎ　Ｅｌｌｉｐｔｉｃ　Ｃｕｒｖｅ　Ｃｒｙｐｔｏｇｒａｐｈｙ（ＥＣＣ　２００１）、

２００１年１０月３０日、［２００２年９月２９日検索］、インターネット＜ＵＲＬ：ｈｔｔｐ：／／ｗｗｗ．ｃａｃｒ．ｍａｔｈ．ｕｗａｔｅｒｌｏｏ．ｃａ／ｃｏｎｆｅｒｅｎｃｅｓ／２００１／ｅｃｃ／ｏｋａｍｏｔｏ．ｐｐｔ＞
【非特許文献５】Ｎｅａｌ　Ｋｏｂｌｉｔｚ，“Ａｌｇｅｂｒａｉｃ　Ａｓｐｅｃｔｓ　ｏｆ　Ｃｒｙｐｔｏｇｒａｐｈｙ”，Ａｌｇｏｒｉｔｈｍｓ　ａｎｄ　Ｃｏｍｐｕｔａｔｉｏｎ　ｉｎ　Ｍａｔｈｅｍａｔｉｃｓ　Ｖｏｌ．３，ｐｐ．１３２－１３３，Ｓｐｒｉｎｇｅｒ－Ｖｅｒｌａｇ，１９９８．
【非特許文献６】Ｍ．　Ｂｅｌｌａｒｅ　ａｎｄ　Ｐ．　Ｒｏｇａｗａｙ，“Ｍｉｎｉｍｉｚｉｎｇ　ｔｈｅ　ｕｓｅ　ｏｆ　ｒａｎｄｏｍ　ｏｒａｃｌｅｓｉｎ　ａｕｔｈｅｎｔｉｃａｔｅｄ　ｅｎｃｒｙｐｔｉｏｎ　ｓｃｈｅｍｅｓ．　Ｉｎ　Ｐｒｏｃｅｅｄｉｎｇｓ　ｏｆ　ＰＫＳ’９７，　１９９７．

【発明の開示】
【発明が解決しようとする課題】
【００１９】
しかしながら、ＤＴＣＰの認証鍵共有方法では安全性の証明がなされておらず、安全性に不安がある。
【００２０】
本発明は、安全性証明がされている暗号方式を利用することで、安全性が保証される認証鍵共有システムを提供することを目的とする。
【課題を解決するための手段】
【００２１】
上記目的を達成するために、請求項１における発明は、第１の機器と第２の機器を備え、前記第１の機器と前記第２の機器との間で鍵配送を行い、共有した鍵を用いて前記第１の機器から前記第２の機器へコンテンツデータを送信する暗号通信システムであって、前記第１の機器は、第１の公開鍵証明書と第１のコンテンツデータを格納する第１のデータ格納部と、前記第２の機器へデータを送信する第１の送信部と、前記第２の機器から送信されたデータを受信する第１の受信部と、第２の公開鍵証明書を検証する第１の証明書検証部と、第１の鍵と第１の鍵を暗号化した第１の暗号化鍵を生成する第１の暗号化鍵生成部と、第２の暗号化鍵から復号化し、復号化した結果を第２の鍵として出力する第１の暗号化鍵復号部と、前記第１の鍵と前記第２の鍵に基づき共有鍵を生成する共有鍵生成部と、前記共有鍵を格納する共有鍵格納部と、前記共有鍵の一部または全部を用いて、前記第１のコンテンツデータを共通鍵暗号を用いて暗号化した第１の暗号化コンテンツデータと、前記共有鍵の一部または全部と鍵付ハッシュ関数を用いて第１のハッシュ値を生成する第１の暗号化部とを含み、前記第２の機器は、前記第２の公開鍵証明書と前記第２のコンテンツデータを格納する第２のデータ格納部と、前記第１の機器へデータを送信する第２の送信部と、前記第１の機器から送信されたデータを受信する第２の受信部と、前記第１の公開鍵証明書を検証する第２の証明書検証部と、第２の鍵と第２の鍵を暗号化した前記第２の暗号化鍵を生成する第２の暗号化鍵生成部と、前記第１の暗号化鍵から復号化し、復号化した結果を前記第１の鍵として出力する第２の暗号化鍵復号部と、前記第１の鍵と前記第２の鍵に基づき共有鍵を生成する前記共有鍵生成部と、前記共有鍵を格納する前記共有鍵格納部と、前記第１の暗号化コンテンツデータを復号化し、第１の復号コンテンツデータを取得し、前記第１の復号コンテンツデータに対して、前記共有鍵の一部または全部と前記鍵付ハッシュ関数を用いて第２のハッシュ値を生成し、前記第１のハッシュ値と比較する第１の復号化部とを含むことを特徴とする。
【００２２】
請求項２における発明は、第１の機器はさらに、第２の暗号化コンテンツデータを復号化し、第２の復号コンテンツデータを取得し、前記第２の復号コンテンツデータに対して、前記共有鍵の一部または全部と前記鍵付ハッシュ関数を用いて第３のハッシュ値を生成し、第４のハッシュ値と比較する第２の復号化部を含み、第２の機器はさらに、前記共有鍵の一部または全部を用いて、前記第２のコンテンツデータを暗号化した前記第２の暗号

化コンテンツデータと、前記共有鍵の一部または全部と鍵付ハッシュ関数を用いて前記第４のハッシュ値を生成する第２の暗号化部を含むことを特徴とする。

【００２３】

請求項３における発明は、前記第１の暗号化鍵及び前記第２の暗号化鍵は、鍵カプセル化メカニズムを用いて生成することを特徴とする。

【００２４】

請求項４における発明は、前記共有鍵生成部は、前記第１の鍵と前記第２の鍵の排他的論理和を前記共有鍵として出力することを特徴とする。

【００２５】

請求項５における発明は、前記共有鍵生成部は、前記第１の鍵と前記第２の鍵をビット連結したものをハッシュ関数を用いて計算したハッシュ値を前記共有鍵として出力することを特徴とする。

【００２６】

請求項６における発明は、第１の機器と第２の機器を備え、前記第１の機器と前記第２の機器との間で鍵配送を行う認証鍵共有システムであって、前記第１の機器は、第１の公開鍵証明書と第１のコンテンツデータを格納する第１のデータ格納部と、前記第２の機器へデータを送信する第１の送信部と、前記第２の機器から送信されたデータを受信する第１の受信部と、第２の公開鍵証明書を検証する第１の証明書検証部と、鍵カプセル化メカニズムを用いて第１の鍵と第１の鍵を暗号化した第１の暗号化鍵を生成する第１の暗号化鍵生成部と、第２の暗号化鍵から復号化し、第２の鍵を出力する第１の暗号化鍵復号部と、前記第１の鍵と前記第２の鍵に基づき共有鍵を生成する共有鍵生成部と、前記共有鍵を格納する共有鍵格納部とを含み、前記第２の機器は、前記第２の公開鍵証明書と前記第２のコンテンツデータを格納する第２のデータ格納部と、前記第１の機器へデータを送信する第２の送信部と、前記第１の機器から送信されたデータを受信する第２の受信部と、前記第１の公開鍵証明書を検証する第２の証明書検証部と、第２の鍵と第２の鍵を暗号化した前記第２の暗号化鍵を生成する第２の暗号化鍵生成部と、前記第１の暗号化鍵から復号化し、前記第１の鍵を出力する第２の暗号化鍵復号部と、前記第１の鍵と前記第２の鍵に基づき共有鍵を生成する前記共有鍵生成部と、前記共有鍵を格納する前記共有鍵格納部とを含むことを特徴とする。

【００２７】

請求項７における発明は、コンテンツ送信機器とコンテンツ受信機器を備え、前記コンテンツ送信機器と前記コンテンツ受信機器との間で鍵配送を行い、共有した鍵を用いて暗号化通信を行う暗号通信システムにおけるコンテンツ送信機器であって、第１の公開鍵証明書と第１のコンテンツデータを格納する第１のデータ格納部と、前記コンテンツ受信機器へデータを送信する第１の送信部と、前記コンテンツ受信機器から送信されたデータを受信する第１の受信部と、前記コンテンツ受信機器に対する第２の公開鍵証明書を検証する第１の証明書検証部と、第１の鍵と第１の鍵を暗号化した第１の暗号化鍵を生成する第１の暗号化鍵生成部と、前記コンテンツ受信機器から送信される第２の暗号化鍵を復号化し、復号化した結果を第２の鍵として出力する第１の暗号化鍵復号部と、前記第１の鍵と前記第２の鍵に基づき共有鍵を生成する共有鍵生成部と、前記共有鍵を格納する共有鍵格納部と、前記共有鍵の一部または全部を用いて、前記第１のコンテンツデータを共通鍵暗号を用いて暗号化した第１の暗号化コンテンツデータと、前記共有鍵の一部または全部と鍵付ハッシュ関数を用いて第１のハッシュ値を生成する第１の暗号化部とを備えることを特徴とする。

【００２８】

請求項８における発明は、前記第１の暗号化鍵は、鍵カプセル化メカニズムを用いて生成することを特徴とする。

【００２９】

請求項９における発明は、前記共有鍵生成部は、前記第１の鍵と前記第２の鍵の排他的論理和を前記共有鍵として出力することを特徴とする。

【００３０】
請求項１０における発明は、前記共有鍵生成部は、前記第１の鍵と前記第２の鍵をビット連結したものをハッシュ関数を用いて計算したハッシュ値を前記共有鍵として出力することを特徴とする。
【００３１】
請求項１１における発明は、コンテンツ送信機器とコンテンツ受信機器を備え、前記コンテンツ送信機器と前記コンテンツ受信機器との間で鍵配送を行い、共有した鍵を用いて暗号化通信を行う暗号通信システムにおけるコンテンツ受信機器であって、第２の公開鍵証明書と第２のコンテンツデータを格納する第２のデータ格納部と、前記コンテンツ送信機器へデータを送信する第２の送信部と、前記コンテンツ送信機器から送信されたデータを受信する第２の受信部と、前記コンテンツ送信機器に対する前記第１の公開鍵証明書を検証する第２の証明書検証部と、第２の鍵と第２の鍵を暗号化した第２の暗号化鍵を生成する第２の暗号化鍵生成部と、前記コンテンツ送信機器から送信された第１の暗号化鍵を復号化し、復号化した結果を第１の鍵として出力する第２の暗号化鍵復号部と、前記第１の鍵と第２の鍵に基づき共有鍵を生成する共有鍵生成部と、前記共有鍵を格納する共有鍵格納部と、前記コンテンツ送信機器から送信された第１の暗号化コンテンツデータを復号化し、第１の復号コンテンツデータを取得し、前記第１の復号コンテンツデータに対して、前記共有鍵の一部または全部と鍵付ハッシュ関数を用いて第２のハッシュ値を生成し、第１のハッシュ値と比較する第１の復号化部とを備えることを特徴とする。
【００３２】
請求項１２における発明は、前記第２の暗号化鍵は、鍵カプセル化メカニズムを用いて生成することを特徴とする。
【００３３】
請求項１３における発明は、前記共有鍵生成部は、前記第１の鍵と前記第２の鍵の排他的論理和を前記共有鍵として出力することを特徴とする。
【００３４】
請求項１４における発明は、前記共有鍵生成部は、前記第１の鍵と前記第２の鍵をビット連結したものをハッシュ関数を用いて計算したハッシュ値を前記共有鍵として出力することを特徴とする。
【００３５】
請求項１５における発明は、第１の機器と第２の機器を備え、前記第１の機器と前記第２の機器との間で鍵配送を行い、共有した鍵を用いて前記第１の機器から前記第２の機器へコンテンツデータを送信する暗号通信方法であって、第１の公開鍵証明書と第１のコンテンツデータを格納する第１のデータ格納ステップと、前記第２の機器へデータを送信する第１の送信ステップと、前記第２の機器から送信されたデータを受信する第１の受信ステップと、第２の公開鍵証明書を検証する第１の証明書検証ステップと、第１の鍵と第１の鍵を暗号化した第１の暗号化鍵を生成する第１の暗号化鍵生成ステップと、第２の暗号化鍵から復号化し、復号化した結果を第２の鍵として出力する第１の暗号化鍵復号ステップと、前記第１の鍵と前記第２の鍵に基づき共有鍵を生成する共有鍵生成ステップと、前記共有鍵を格納する共有鍵格納ステップと、前記共有鍵の一部または全部を用いて、前記第１のコンテンツデータを共通鍵暗号を用いて暗号化した第１の暗号化コンテンツデータと、前記共有鍵の一部または全部と鍵付ハッシュ関数を用いて第１のハッシュ値を生成する第１の暗号化ステップとを前記第１の機器に実行させ、前記第２の公開鍵証明書と前記第２のコンテンツデータを格納する第２のデータ格納ステップと、前記第１の機器へデータを送信する第２の送信ステップと、前記第１の機器から送信されたデータを受信する第２の受信ステップと、前記第１の公開鍵証明書を検証する第２の証明書検証ステップと、第２の鍵と第２の鍵を暗号化した前記第２の暗号化鍵を生成する第２の暗号化鍵生成ステップと、前記第１の暗号化鍵から復号化し、復号化した結果を前記第１の鍵として出力する第２の暗号化鍵復号ステップと、前記共有鍵生成ステップと、前記共有鍵格納ステップと、前記第１の暗号化コンテンツデータを復号化し、第１の復号コンテンツデータを取得

し、前記第１の復号コンテンツデータに対して、前記共有鍵の一部または全部と前記鍵付ハッシュ関数を用いて第２のハッシュ値を生成し、前記第１のハッシュ値と比較する第１の復号化ステップとを前記第２の機器に実行させることを特徴とする。

【００３６】

請求項１６における発明は、第１の機器はさらに、第２の暗号化コンテンツデータを復号化し、第２の復号コンテンツデータを取得し、前記第２の復号コンテンツデータに対して、前記共有鍵の一部または全部と前記鍵付ハッシュ関数を用いて第３のハッシュ値を生成し、第４のハッシュ値と比較する第２の復号化ステップを含み、第２の機器はさらに、前記共有鍵の一部または全部を用いて、前記第２のコンテンツデータを暗号化した前記第２の暗号化コンテンツデータと、前記共有鍵の一部または全部と鍵付ハッシュ関数を用いて前記第４のハッシュ値を生成する第２の暗号化ステップを含むことを特徴とする。

【００３７】

請求項１７における発明は、前記第１の暗号化鍵及び前記第２の暗号化鍵は、鍵カプセル化メカニズムを用いて生成することを特徴とする。

【００３８】

請求項１８における発明は、コンテンツ送信機器とコンテンツ受信機器を備え、前記コンテンツ送信機器と前記コンテンツ受信機器との間で鍵配送を行い、共有した鍵を用いて暗号化通信を行う暗号通信システムにおけるコンテンツ送信機器で実行されるプログラムであって、第１の公開鍵証明書と第１のコンテンツデータを格納する第１のデータ格納ステップと、前記コンテンツ受信機器へデータを送信する第１の送信ステップと、前記コンテンツ受信機器から送信されたデータを受信する第１の受信ステップと、前記コンテンツ受信機器に対する第２の公開鍵証明書を検証する第１の証明書検証ステップと、第１の鍵と第１の鍵を暗号化した第１の暗号化鍵を生成する第１の暗号化鍵生成ステップと、前記コンテンツ受信機器から送信される第２の暗号化鍵を復号化し、復号化した結果を第２の鍵として出力する第１の暗号化鍵復号ステップと、前記第１の鍵と前記第２の鍵に基づき共有鍵を生成する共有鍵生成ステップと、前記共有鍵を格納する共有鍵格納ステップと、前記共有鍵の一部または全部を用いて、前記第１のコンテンツデータを共通鍵暗号を用いて暗号化した第１の暗号化コンテンツデータと、前記共有鍵の一部または全部と鍵付ハッシュ関数を用いて第１のハッシュ値を生成する第１の暗号化ステップとをコンテンツ送信機器に実行させることを特徴とする。

【００３９】

請求項１９における発明は、コンテンツ送信機器とコンテンツ受信機器を備え、前記コンテンツ送信機器と前記コンテンツ受信機器との間で鍵配送を行い、共有した鍵を用いて暗号化通信を行う暗号通信システムにおけるコンテンツ受信機器で実行されるプログラムであって、第２の公開鍵証明書と第２のコンテンツデータを格納する第２のデータ格納ステップと、前記コンテンツ送信機器へデータを送信する第２の送信ステップと、前記コンテンツ送信機器から送信されたデータを受信する第２の受信ステップと、前記コンテンツ送信機器に対する前記第１の公開鍵証明書を検証する第２の証明書検証ステップと、第２の鍵と第２の鍵を暗号化した第２の暗号化鍵を生成する第２の暗号化鍵生成ステップと、前記コンテンツ送信機器から送信された第１の暗号化鍵を復号化し、復号化した結果を前記第１の鍵として出力する第２の暗号化鍵復号ステップと、前記第１の鍵と前記第２の鍵に基づき共有鍵を生成する共有鍵生成ステップと、前記共有鍵を格納する共有鍵格納ステップと、前記コンテンツ送信機器から送信された第１の暗号化コンテンツデータを復号化し、第１の復号コンテンツデータを取得し、前記第１の復号コンテンツデータに対して、前記共有鍵の一部または全部と前記鍵付ハッシュ関数を用いて第２のハッシュ値を生成し、前記第１のハッシュ値と比較する第１の復号化ステップとをコンテンツ受信機器に実行させることを特徴とする。

【００４０】

請求項２０における発明は、請求項１８または１９に記載のプログラムを記録した媒体。

【発明の効果】
【００４１】
これらの構成によると、鍵カプセル化メカニズム、共通鍵暗号と鍵付ハッシュ関数を用いることにより、安全性を保証でき、双方向で暗号化鍵を送りあうことにより、認証鍵共有を実現できるため、その価値は大きい。
【発明を実施するための最良の形態】
【００４２】
（実施の形態１）
本発明にかかる実施の形態１としての暗号通信システム１０００について説明する。
【００４３】
図１は、実施の形態１における暗号通信システム１０００の構成を示す図である。本システムは、機器Ａ１１００、機器Ｂ１２００から構成される。
【００４４】
＜機器Ａ１１００の構成＞
機器Ａ１１００は、データを保持するデータ格納部１１０１と、データを送信する送信部１１０２と、情報を受信する受信部１１０３と、証明書を検証する証明書検証部１１０４と、秘密鍵ＫＳＡを格納する秘密鍵格納部１１０５と、暗号化鍵を生成する暗号化鍵生成部１１０６と、暗号化鍵を復号する暗号化鍵復号部１１０７と、共有鍵を生成する共有鍵生成部１１０８と、共有鍵を格納する共有鍵格納部１１０９と、コンテンツデータを暗号化する暗号化部１１１０と、コンテンツデータを復号化する復号化部１１１１とを備える。
【００４５】
データ格納部１１０１は、証明書Ｃｅｒｔ＿Ａ、センタ署名検証鍵ＫＰＣ及びコンテンツデータＤＡを保持する。ここで、Ｃｅｒｔ＿Ａは公開鍵ＫＰＡとそのセンタ署名ＳＫＰＡ＝Ｓｉｇ（ＫＳＣ，ＫＰＡ）からなる。なお、Ｃｅｒｔ＿Ａに他データ例えば、ＩＤ情報が含まれてもよいし、センタ署名ＳＫＰＡがＫＰＡと他のデータ、例えば、ＩＤ情報との連結に対する署名であってもよい。ＫＳＣはセンタ署名検証鍵ＫＰＣに対するセンタ署名生成鍵であり、Ｓｉｇ（ＫＳＣ，ＫＰＡ）はセンタ署名生成鍵ＫＳＣを用いたＫＰＡの署名を意味する。なお、証明書Ｃｅｒｔ＿Ａ及びセンタ署名検証鍵ＫＰＣは、予め証明書センタが作成して配布されているものとする。ここで使用する署名方式は、例えばＲＳＡ署名、楕円ＤＳＡ署名である。署名方式については、非特許文献２が詳しい。
【００４６】
送信部１１０２は、機器Ｂ１２００へデータを送信する。
【００４７】
受信部１１０３は、機器Ｂ１２００から送信されたデータを受信する。
【００４８】
証明書検証部１１０４は、機器Ｂ１２００の公開鍵ＫＰＢの証明書Ｃｅｒｔ＿Ｂに含まれている公開鍵ＫＰＢとそのセンタ署名ＳＫＰＢに対し、データ格納部１１０１に格納されているセンタ署名検証鍵ＫＰＣを用いて、センタ署名ＳＫＰＢが公開鍵ＫＰＢの正しい署名であるか署名検証する。
【００４９】
秘密鍵格納部１１０５は、秘密鍵ＫＳＡを秘密に格納する。
【００５０】
暗号化鍵生成部１１０６は、鍵ＫＡとその暗号化鍵ＫＥＭＡを生成する。この鍵ＫＡ及び暗号化鍵ＫＥＭＡは、鍵配送方式の一種である鍵カプセル化メカニズム（Ｋｅｙ　Ｅｎｃａｐｓｕｌａｔｉｏｎ　Ｍｅｃｈａｎｉｓｍｓ）と呼ばれる方式を用いて作成する。鍵カプセル化メカニズムについては、非特許文献３が詳しい。鍵カプセル化メカニズムについては、機器Ａ１１００内の各部の説明をした後で詳しく述べる。
【００５１】
暗号化鍵復号部１１０７は、機器Ｂ１２００より送信される暗号化鍵ＫＥＭＢを復号化

し、鍵ＫＢを出力する。暗号化鍵ＫＥＭＢは、先に述べた鍵カプセル化メカニズムにより、作成されている。そのため、ここでの復号化も、鍵カプセル化メカニズムの復号化を用いて行う。

【００５２】

共有鍵生成部１１０８は、鍵ＫＡ及び鍵ＫＢより、共通鍵暗号用共有鍵ＫＳとハッシュ用共有鍵ＫＨを生成する。具体的には、例えば、鍵ＫＡとＫＢの排他的論理和を取り、その一部を共有鍵暗号用共有鍵ＫＳとし、それ以外の部分をハッシュ用共有鍵ＫＨとする。この方法は、鍵ＫＡとＫＢの両方の一部または全部の情報がＫＳ、ＫＨに含まれるものであればよい。

【００５３】

共有鍵格納部１１０９は、共通鍵暗号用共有鍵ＫＳとハッシュ用共有鍵ＫＨを格納する。

【００５４】

データ暗号化部１１１０は、コンテンツデータＤＡを共通鍵暗号用共有鍵ＫＳを用いて暗号化し、Ｅｎｃ（ＫＳ，ＤＡ）を作成し、ハッシュ用共有鍵ＫＨを用いて、ハッシュ値Ｈａｓｈ（ＫＨ，ＤＡ）。ここで、Ｅｎｃ（ＫＳ，ＤＡ）は鍵ＫＳを用いてＤＡを共通鍵暗号で暗号化した暗号文であり、Ｈａｓｈ（ＫＨ，ＤＡ）は鍵ＫＨを用いて、鍵付ハッシュ関数で計算したＤＡのハッシュ値を意味する。共通鍵暗号は例えばＤＥＳ暗号やＡＥＳ暗号である。また、Ｈａｓｈ（ＫＨ，ＤＡ）は、Ｈａｓｈ（ＫＨ，ＤＡ）＝ＳＨＡ１（ＫＨ｜｜ＤＡ）としてもよい。ここで、ＳＨＡ１（ｘ）は、ｘのＳＨＡ１ハッシュ関数値であり、｜｜は連結を示す。共通鍵暗号及び鍵付ハッシュ関数については、非特許文献２が詳しい。

【００５５】

データ復号化部１１１１は、コンテンツデータＤＢの暗号文ＣＤＢ＝Ｅｎｃ（ＫＳ，ＤＢ）を復号化して、データＤＢ’を取得し、データＤＢ’のハッシュ値ＨＤＢ’＝Ｈａｓｈ（ＫＨ、ＤＢ’）を計算し、ＨＤＢと比較する。

【００５６】

（鍵カプセル化メカニズム）

以下で鍵カプセル化メカニズムについて詳しく述べる。

【００５７】

鍵カプセル化メカニズムは、簡単に説明すると、公開鍵暗号を用いて送信装置と受信装置の間で共有鍵を配送するアルゴリズムであり、送信側が、公開鍵暗号化アルゴリズムＥに受信者の公開鍵ｐｋを入力して暗号文Ｃと共有鍵Ｋを生成し、暗号文Ｃを受信側に伝送する。そして、受信側が、公開鍵復号アルゴリズムＤに、秘密鍵ｓｋと暗号文Ｃを入力して送信側と同じ共有鍵Ｋを求める方式である。

【００５８】

鍵カプセル化メカニズムの目的は、鍵カプセル化メカニズムで共有鍵Ｋを送信装置と受信装置で共有することにより、その後、送信装置から受信装置へ通信される通信内容データを、共有鍵Ｋを用いて共通鍵暗号で暗号化することにある。ここで、送信者から受信者に一方的に情報の送信が行われていながら、送信者が作為的に共有鍵を作成できず、送信者による不正が抑制されている点が従来の鍵配送方式にない特徴である。

【００５９】

このような鍵カプセル化メカニズムとして、ＰＳＥＣ－ＫＥＭと呼ばれるアルゴリズムが開示されている（例えば、非特許文献４参照）。以下に、この非特許文献４に記載されているＰＳＥＣ－ＫＥＭアルゴリズムについて説明する。

【００６０】

（１）ＰＳＥＣ－ＫＥＭのシステムパラメータ

ＰＳＥＣ－ＫＥＭは、以下のシステムパラメータを持つ。

【００６１】

・楕円曲線：Ｅ

・楕円曲線上の位数ｎの点：Ｐ
・ハッシュ関数：Ｇ，Ｈ
なお、楕円曲線、位数及びハッシュ関数については、非特許文献２に詳細が記述されているので、ここでは説明を省略する。
【００６２】
（２）ＰＳＥＣ－ＫＥＭの公開鍵と秘密鍵
・ランダムにＺｎの要素ｘを選び、Ｗ＝ｘ＊Ｐを生成する。
【００６３】
ここで、Ｚｎは、｛０，１，．．．，ｎ－１｝からなる集合であり、ｘ＊Ｐは、楕円曲線上の点Ｐをｘ回加算することにより得られる楕円曲線上の点を表す。なお、楕円曲線上の点の加算方法については、非特許文献２に記述されている。
【００６４】
・公開鍵ｐｋを（Ｅ，Ｐ，Ｗ，ｎ）とし、秘密鍵ｓｋをｘとする。
【００６５】
（３）ＰＳＥＣ－ＫＥＭの暗号化
暗号化時には、以下に述べる公開鍵暗号化アルゴリズムＫｅｍＥに公開鍵ｐｋを入力して共有鍵Ｋと暗号文Ｃを出力する。以下に公開鍵暗号化アルゴリズムＫｅｍＥについて説明する。
【００６６】
・Ｚｎの要素ｓをランダムに生成する。
【００６７】
・Ｇ（ｓ）を生成し、Ｇ（ｓ）をＧ（ｓ）＝ａ｜｜Ｋと分割する。ここで、｜｜はビット結合を表し，Ｇ（ｓ）をＧ（ｓ）＝ａ｜｜Ｋと分割するとは、Ｇ（ｓ）の上位複数ビットをａとし、残りのビットをＫとすることを表す。
【００６８】
・Ｒ＝ａ＊Ｐ，Ｑ＝ａ＊Ｗを生成する。
【００６９】
・ｖ＝ｓ　ｘｏｒ　Ｈ（Ｒ｜｜Ｑ）を生成する。ここで、ｘｏｒは排他的論理和演算を表す。
【００７０】
・共有鍵Ｋと暗号文Ｃ＝（Ｒ，ｖ）を出力する。
【００７１】
（４）ＰＳＥＣ－ＫＥＭの復号化
復号化時には、以下に述べる公開鍵復号アルゴリズムＫｅｍＤに暗号文Ｃ＝（Ｒ，ｖ）と公開鍵ｐｋと秘密鍵ｓｋを入力して共有鍵Ｋを出力する。以下に復号アルゴリズムＫｅｍＤについて説明する。
【００７２】
・Ｑ＝ｘ＊Ｒを生成する。
【００７３】
・ｓ’＝ｖ　ｘｏｒ　Ｈ（Ｒ｜｜Ｑ）を生成する。
【００７４】
・Ｇ（ｓ’）を生成し、Ｇ（ｓ’）をＧ（ｓ’）＝ａ｜｜Ｋと分割する。
【００７５】
・Ｒ＝ａ＊Ｐが成立するかどうかチェックする。成立すれば共有鍵Ｋを出力する。
【００７６】
このＰＳＥＣ－ＫＥＭアルゴリズムを、送信装置と受信装置の間で暗号化通信を行う暗号システムに応用した場合、まず、送信装置は、通信先受信装置の公開鍵ｐｋを取得し、取得した公開鍵ｐｋを前述の公開鍵暗号化アルゴリズムＫｅｍＥに入力して共有鍵Ｋと暗号文Ｃを導出して、暗号文Ｃを受信装置へ送信する。そして、受信装置は、送信装置から暗号文Ｃを受信し、受信した暗号文Ｃと自身が有する公開鍵ｐｋ・秘密鍵ｓｋを前述の公

開鍵復号アルゴリズムＫｅｍＤに入力して、送信装置が導出したものと等しい共有鍵Ｋを導出する。

【００７７】

以下に、このことを詳細に説明する。

【００７８】

今、ＰＳＥＣ－ＫＥＭアルゴリズムは、ハッシュ関数Ｈの入力を（ａ＊Ｐ｜｜ａ＊Ｗ）としており、公開鍵暗号化アルゴリズムＫｅｍＥで、ランダムに生成した要素ｓにＨ（ａ＊Ｐ｜｜ａ＊Ｗ）の値を作用させてｖを生成する。そして、公開鍵復号アルゴリズムＫｅｍＤでは、Ｒ＝ａ＊Ｐから秘密鍵ｓｋ（＝ｘ）を用いてＱ＝ｘ＊Ｒ＝ｘ＊（ａ＊Ｐ）＝ａ＊（ｘ＊Ｐ）＝ａ＊Ｗを求めることができるので、ｖ　ｘｏｒ　Ｈ（ａ＊Ｐ｜｜ａ＊Ｗ）を計算することにより、公開鍵暗号化アルゴリズムＫｅｍＥにおいて生成されたランダムな要素ｓを求めることができる。従って、公開鍵暗号化アルゴリズムＫｅｍＥと公開鍵復号アルゴリズムＫｅｍＤは、ハッシュ関数Ｇに同じｓの値を入力することができ、同じ共有鍵Ｋを導出することができる。この結果、秘密鍵ｓｋを有する受信装置は、送信装置が導出したものと同じ共有鍵Ｋを導出できることになる。

【００７９】

一方で、秘密鍵ｓｋを知らない他の受信装置は、たとえ公開鍵ｐｋを取得して暗号文Ｃを受信したとしても、秘密鍵ｓｋ（＝ｘ）を知らないのでＲ＝ａ＊ＰからＱ＝ａ＊Ｗ（＝（ａｘ）＊Ｐ）を計算できず、送信装置が導出したものと同じ共有鍵Ｋを導出できない。なぜならば、秘密鍵ｓｋを知らない他の受信装置は、公開鍵ｐｋしか利用できないので、上記Ｑの計算には秘密鍵ｓｋ（＝ｘ）の代わりに公開鍵ｐｋのＷ＝ｘ＊Ｐを利用することになるが、一般に、ａ＊ＰとＷ＝ｘ＊Ｐから、Ｑ＝ａ＊Ｗ（＝（ａｘ）＊Ｐ）を求めることは、楕円曲線上のＤｉｆｆｉｅ－Ｈｅｌｌｍａｎ問題と呼ばれ、ａやｘの値を知らない限り計算困難だからである（例えば、非特許文献５参照）。

【００８０】

すなわち、ＰＳＥＣ－ＫＥＭアルゴリズムは、秘密鍵を用いずにａ＊Ｐからａ＊Ｗを計算することが困難なＤｉｆｆｉｅ－Ｈｅｌｌｍａｎ問題を用いて、最終的に共有鍵Ｋを導出することにより、秘密鍵を知らなければその共有鍵Ｋを導出できないようにしている。

【００８１】

よって、以上により、送信装置と受信装置とは、共有鍵Ｋを秘密に共有することができ、この後、秘密鍵暗号を用いて、送信装置から受信装置へ通信される通信内容データを、共有鍵Ｋを用いて共通鍵暗号で暗号化することができる。

【００８２】

上記のＰＳＥＣ－ＫＥＭアルゴリズムは、先に述べた楕円曲線上のＤｉｆｆｉｅ－Ｈｅｌｌｍａｎ問題が困難であれば、秘密鍵を知らない受信装置は共有鍵Ｋを得ることができないことが証明されている。このような証明を方式の安全性を証明していることから、「安全性証明」と呼ぶ。ＰＳＥＣ－ＫＥＭの他のＫＥＭアルゴリズム、例えばＲＳＡ－ＫＥＭ（非特許文献１参照）なども同様の困難な数学上の問題を根拠として安全性証明されている。

【００８３】

＜機器Ｂ１２０の構成＞

機器Ｂ１２００は、データを保持するデータ格納部１２０１と、データを送信する送信部１２０２と、情報を受信する受信部１２０３と、証明書を検証する証明書検証部１２０４と、秘密鍵ＫＳＢを格納する秘密鍵格納部１２０５と、暗号化鍵を生成する暗号化鍵生成部１２０６と、暗号化鍵を復号する暗号化鍵復号部１２０７と、共有鍵を生成する共有鍵生成部１２０８と、共有鍵を格納する共有鍵格納部１２０９と、コンテンツデータを暗号化する暗号化部１２１０と、コンテンツデータを復号化する復号化部１２１１とを備える。

【００８４】

データ格納部１２０１は、公開鍵ＫＰＢ、その証明書Ｃｅｒｔ＿Ｂ、センタ署名検証鍵

ＫＰＣ及びコンテンツデータＤＢを保持する。なお、証明書Ｃｅｒｔ＿Ｂ及びセンタ署名検証鍵は、予め証明書センタが作成して配布されているものとする。

【００８５】

送信部１２０２は、機器Ａ１１００へデータを送信する。

【００８６】

受信部１２０３は、機器Ａ１１００から送信されたデータを受信する。

【００８７】

証明書検証部１２０４は、機器Ｂ１１００の公開鍵ＫＰＡの証明書Ｃｅｒｔ＿Ａに含まれている公開鍵ＫＰＡとそのセンタ署名ＳＫＰＡに対し、データ格納部１２０１に格納されているセンタ署名検証鍵ＫＰＣを用いて、センタ署名ＳＫＰＡが公開鍵ＫＰＡの正しい署名であるか署名検証する。

【００８８】

秘密鍵格納部１２０５は、秘密鍵ＫＳＢを秘密に格納する。

【００８９】

暗号化鍵生成部１２０６は、鍵ＫＢとその暗号化鍵ＫＥＭＢを生成する。この鍵ＫＢ及び暗号化鍵ＫＥＭＢは、暗号化鍵生成部１１０６と同様、鍵カプセル化メカニズムを用いて作成する。

【００９０】

暗号化鍵復号部１２０７は、機器Ａ１１００から送信される暗号化鍵ＫＥＭＡを復号化し、鍵ＫＡを出力する。暗号化鍵ＫＥＭＡは、先に述べた鍵カプセル化メカニズムにより、作成されている。そのため、ここでの復号化も、鍵カプセル化メカニズムの復号化を用いて行う。

【００９１】

共有鍵生成部１２０８は、鍵ＫＡ及び鍵ＫＢより、共通鍵暗号用共有鍵ＫＳとハッシュ用共有鍵ＫＨを生成する。具体的には、例えば、鍵ＫＡとＫＢの排他的論理和を取り、その一部を共有鍵暗号用共有鍵ＫＳとし、それ以外をハッシュ用共有鍵ＫＨとする。この方法は、鍵ＫＡとＫＢの両方の一部または全部の情報がＫＳ、ＫＨに含まれるものであればよい。

【００９２】

共有鍵格納部１２０９は、共通鍵暗号用共有鍵ＫＳとハッシュ用共有鍵ＫＨを格納する。

【００９３】

データ暗号化部１２１０は、コンテンツデータＤＢを、共通鍵暗号用共有鍵ＫＳを用いて暗号化し、Ｅｎｃ（ＫＳ，ＤＢ）を作成し、ハッシュ用共有鍵ＫＨを用いて、ハッシュ値Ｈａｓｈ（ＫＨ，ＤＢ）。ここで、Ｅｎｃ（ＫＳ，ＤＢ）は鍵ＫＳを用いてＤＡを共通鍵暗号で暗号化した暗号文であり、Ｈａｓｈ（ＫＨ，ＤＢ）は鍵ＫＨを用いて、鍵付ハッシュ関数で計算したＤＢのハッシュ値を意味する。共通鍵暗号は例えばＤＥＳ暗号やＡＥＳ暗号である。また、Ｈａｓｈ（ＫＨ，ＤＢ）は、Ｈａｓｈ（ＫＨ，ＤＢ）＝ＳＨＡ１（ＫＨ｜｜ＤＢ）としてもよい。

【００９４】

復号化部１２１１は、コンテンツデータＤＡの暗号文ＣＤＡ＝Ｅｎｃ（ＫＳ，ＤＡ）を復号化して、データＤＡ’を取得し、データＤＡ’のハッシュ値ＨＤＡ’＝Ｈａｓｈ（ＫＨ，ＤＡ’）を計算し、ＨＤＡと比較する。

【００９５】

＜暗号通信システム１００の動作＞

暗号通信システムでは、機器Ａ１１００と機器Ｂ１２００とが相互認証を行い、鍵共有を行った後、共有した鍵を用いて機器Ａ１１０と機器Ｂ１２０の間でコンテンツデータを送信し合う。ここで、コンテンツデータとは、例えば、テキストデータ、音楽データ、画像データ、映画コンテンツデータである。以下でその動作を示す（図２及び図３参照）。

【００９６】

ステップＳ１０１：機器Ｂ１２００内の送信部１２０２は、データ格納部１２０１に格納されている、証明書Ｃｅｒｔ＿Ｂを、機器Ａ１１００に送信する。

【００９７】

ステップＳ１０２：機器Ａ１１００内の受信部１１０３は、証明書Ｃｅｒｔ＿Ｂを受信する。

【００９８】

ステップＳ１０３：機器Ａ１１００内の証明書検証部１１０４は、証明書Ｃｅｒｔ＿Ｂに含まれる公開鍵ＫＰＢ及びその署名ＳＫＰＢに対して、署名ＳＫＰＢが公開鍵ＫＰＢの正しいセンタ署名であるか否かを、データ格納部１１０１に格納されているセンタ公開鍵ＫＰＣを用いて、検証する。正しいセンタ署名でない場合は、システムを終了させる。正しいセンタ署名の場合は、次のステップＳ１０４へ進む。

【００９９】

ステップＳ１０４：機器Ａ１１００内の暗号化鍵生成部１１０６は、鍵ＫＡと鍵情報ＫＥＭＡを作成する。

【０１００】

ステップＳ１０５：機器Ａ１１００内の送信部１１０２は、データ格納部１１０１に格納されている、公開鍵ＫＰＡ及びその証明書Ｃｅｒｔ＿Ａと、鍵情報ＫＥＭＡを機器Ｂ１２００へ送信する。

【０１０１】

ステップＳ１０６：機器Ｂ１２００内の受信部１２０３は、公開鍵ＫＰＡ、その証明書Ｃｅｒｔ＿Ａと鍵情報ＫＥＭＡを受信する。

【０１０２】

ステップＳ１０７：機器Ｂ１２００内の証明書検証部１２０４は、証明書Ｃｅｒｔ＿Ａに含まれる公開鍵ＫＰＡ及びその署名ＳＫＰＡに対して、署名ＳＫＰＡが公開鍵ＫＰＡの正しいセンタ署名であるか否かを、データ格納部１２０１に格納されているセンタ公開鍵ＫＰＣを用いて、検証する。正しいセンタ署名でない場合は、システムを終了させる。正しいセンタ署名の場合は、次のステップＳ１０８へ進む。

【０１０３】

ステップＳ１０８：機器Ｂ１２００内の暗号化鍵復号部１２０７は、秘密鍵格納部１２０５より秘密鍵ＫＳＢを取得し、秘密鍵ＫＳＢを用いて、鍵情報ＫＥＭＡより、鍵ＫＡを復号化する。

【０１０４】

ステップＳ１０９：機器Ｂ１２００内の暗号化鍵生成部１２０６は、鍵ＫＢと鍵情報ＫＥＭＢを作成する。

【０１０５】

ステップＳ１１０：機器Ｂ１２００内の送信部１２０２は、鍵情報ＫＥＭＢを機器Ａ１１００へ送信する。

【０１０６】

ステップＳ１１１：機器１１００内の受信部１１０３は、鍵情報ＫＥＭＢを受信する。

【０１０７】

ステップＳ１１２：機器１１００内の暗号化鍵復号部１１０７は、秘密鍵格納部１１０５より秘密鍵ＫＳＡを取得し、秘密鍵ＫＳＢを用いて、鍵情報ＫＥＭＢより、鍵ＫＢを復号化する。

【０１０８】

ステップＳ１１３：機器Ｂ１２００内の共有鍵生成部１２０８は、鍵ＫＢと復号した鍵ＫＡを用いて、共通鍵暗号用共有鍵ＫＳと鍵付ハッシュ用共有鍵ＫＨを計算し、それぞれを共有鍵格納部１２０９に格納する。

【０１０９】

ステップＳ１１４：機器Ａ１１００内の共有鍵生成部１１０８は、鍵ＫＡと復号した鍵ＫＡを用いて、共通鍵暗号用共有鍵ＫＳと鍵付ハッシュ用共有鍵ＫＨを計算し、それぞれ

を共有鍵格納部１１０９に格納する。

【０１１０】

ステップＳ１１５：機器Ａ１１００内の暗号化部１１１０は、データ格納部１１０１に格納されているコンテンツデータＤＡを、共通鍵暗号用共有鍵ＫＳを用いて暗号化して暗号化コンテンツデータＣＤＡを作成する。さらに暗号化部１１１０は、鍵付ハッシュ用共有鍵ＫＨを用いて、コンテンツデータＤＡのハッシュ値ＨＤＡを計算する。

【０１１１】

ステップＳ１１６：機器Ａ１１００内の送信部１１０２は、暗号化コンテンツデータＣＤＡとハッシュ値ＨＤＡを機器Ｂ１２００へ送信する。

【０１１２】

ステップＳ１１７：機器Ｂ１２００内の受信部１２０３は、暗号化コンテンツデータＣＤＡを受信する。

【０１１３】

ステップＳ１１８：機器Ｂ１２００内の復号化部１２１１は、暗号化コンテンツデータＣＤＡを復号して復号コンテンツデータＤＡ’を取得する。さらに復号化部１２１１は、鍵付ハッシュ用共有鍵ＫＨを用いて、復号コンテンツデータＤＡ’のハッシュ値ＨＤＡ’を計算し、ＨＤＡと比較する。ＨＤＡ≠ＨＤＡ’であれば、システムを終了させる。それ以外は復号コンテンツデータＤＡ’をデータ格納部１２０１に格納する。

【０１１４】

ステップＳ１１９：機器Ｂ１２００内の暗号化部１２１０は、データ格納部１２０１に格納されているコンテンツデータＤＢを、共通鍵暗号用共有鍵ＫＳを用いて暗号化して暗号化コンテンツデータＣＤＢを作成する。さらに暗号化部１２１０は、鍵付ハッシュ用共有鍵ＫＨを用いて、コンテンツデータＤＢのハッシュ値ＨＤＢを計算する。

【０１１５】

ステップＳ１２０：機器Ｂ１２００内の送信部１２０２は、暗号化コンテンツデータＣＤＢとハッシュ値ＨＤＢを機器Ａ１１００へ送信する。

【０１１６】

ステップＳ１２１：機器Ａ１１００内の受信部１１０３は、暗号化コンテンツデータＣＤＢを受信する。

【０１１７】

ステップＳ１２２：機器Ａ１１００内の復号化部１１１１は、暗号化コンテンツデータＣＤＢを復号して復号コンテンツデータＤＢ’を取得する。さらに復号化部１１１１は、鍵付ハッシュ用共有鍵ＫＨを用いて、復号コンテンツデータＤＢ’のハッシュ値ＨＤＢ’を計算し、ＨＤＢと比較する。ＨＤＢ≠ＨＤＢ’であれば、システムを終了させる。それ以外は復号コンテンツデータＤＢ’をデータ格納部１１０１に格納し、終了する。

【０１１８】

（実施の形態１の効果）

鍵カプセル化メカニズムで共有した鍵を用いて、データに対して、暗号化した暗号化データとそのデータに対する鍵付ハッシュ関数値を送信するような方式であれば、データ暗号化方法として、困難な数学上の問題を根拠にして安全性証明を可能であることが保証されている（非特許文献３参照）。本方式は、同様に、鍵カプセル化メカニズムで共有した鍵を用いて、コンテンツデータに対して、暗号化した暗号化コンテンツデータとそのコンテンツデータに対する鍵付ハッシュ値を送信しているため、同様の安全性が保証できる。また、機器Ａ１１００において、正しい秘密鍵ＫＳＡを保持していなければ、暗号化鍵ＫＥＭＢを復号化して鍵ＫＢを取得できないため、機器Ｂ１２００と共有した共通鍵暗号用共有鍵ＫＳ及び鍵付ハッシュ用共有鍵ＫＨを得られない。そのため、ステップＳ１２２におけるデータ復号化ができない。また、機器Ｂ１２００も同様に、正しい秘密鍵ＫＳＢを保持していなければ、暗号化鍵ＫＥＭＡを復号化して鍵ＫＡを取得できないため、機器Ａ１１００と共有した共通鍵暗号用共有鍵ＫＳ及び鍵付ハッシュ用共有鍵ＫＨを得られない。そのため、ステップＳ１１８のデータ復号化ができない。正しく鍵ＫＡまたは、鍵ＫＢ

を取得するためには、正しい秘密鍵ＫＳＡまたは、ＫＳＢが必要である。したがって、両方の機器から暗号化鍵ＫＥＭＢ，ＫＥＭＡを送りあうことにより、双方向の認証が実現できている。また、当然ながら、共有鍵を共有できているため、認証鍵共有が実現できている。以上より、安全性を保証できる認証鍵共有を実現でき、その価値は大きい。

【０１１９】

（変形例）

上記に説明した実施の形態は、本発明の実施の一例であり、本発明はこの実施の形態に何ら限定されるものではなく、その旨を逸脱しない範囲において種々なる態様で実施し得るものである。例えば、以下のような場合も本発明に含まれる。

【０１２０】

（１）機器Ａ１１００及び機器Ｂ１２００からコンテンツデータを送り合うが、これが一方、例えば機器Ａ１１００のみからコンテンツデータを送るとしてもよい。

【０１２１】

（２）共有鍵を共有した後、すぐにコンテンツデータを送信しているが、何らかの処理、例えば、機器の機能（音楽視聴機能、映画視聴機能や放送受信機能など）の確認処理が途中に含まれてもよい。

【０１２２】

（３）データ格納部に公開鍵、証明書及びコンテンツデータが格納されているとしたが、データ格納部が複数あり、これらのデータが別々に格納されているとしてもよい。

【０１２３】

（４）送られたコンテンツデータをデータ格納部に格納しているが、コンテンツデータが例えば、画像データであれば、画面に出力、音楽データあれば、スピーカより出力するとしてもよい。

【０１２４】

（５）実施の形態１では、証明書Ｃｅｒｔ＿Ａを公開鍵ＫＰＡとそのセンタ署名Ｓｉｇ（ＫＳＣ，ＫＰＡ）としているが、これに他データ、例えば、ＩＤ情報を付加してもよい。また、センタ署名の対象データであるＫＰＡも、ＫＰＡと他のデータ、例えば、ＩＤ情報との連結としてもよい。

【０１２５】

（６）実施の形態１では、共有鍵生成部で生成する共通鍵暗号用共有鍵ＫＳと鍵付ハッシュ用共有鍵ＫＨは、鍵ＫＡと鍵ＫＢの排他的論理和の一部であるが、これだけには限らない。例えば、鍵ＫＡと鍵ＫＢの連結に対するハッシュ関数値の一部としてもよい。

【産業上の利用可能性】

【０１２６】

これらの構成によると、鍵カプセル化メカニズム、共通鍵暗号と鍵付ハッシュ関数を用いることにより、安全性を保証でき、双方向で暗号化鍵を送り合うことにより、認証鍵共有を実現でき、例えば、コンテンツデータを送受信する装置における暗号技術として有用である。

【図面の簡単な説明】

【０１２７】

【図１】本発明に係る１個の実施の形態としての暗号通信システム１０００の構成を示すシステム構成図

【図２】暗号通信システム１０００の動作を示すフローチャート

【図３】暗号通信システム１０００の動作を示すフローチャート

【図４】従来例であるＤＴＣＰの認証鍵共有方法の動作フロー図

【符号の説明】

【０１２８】

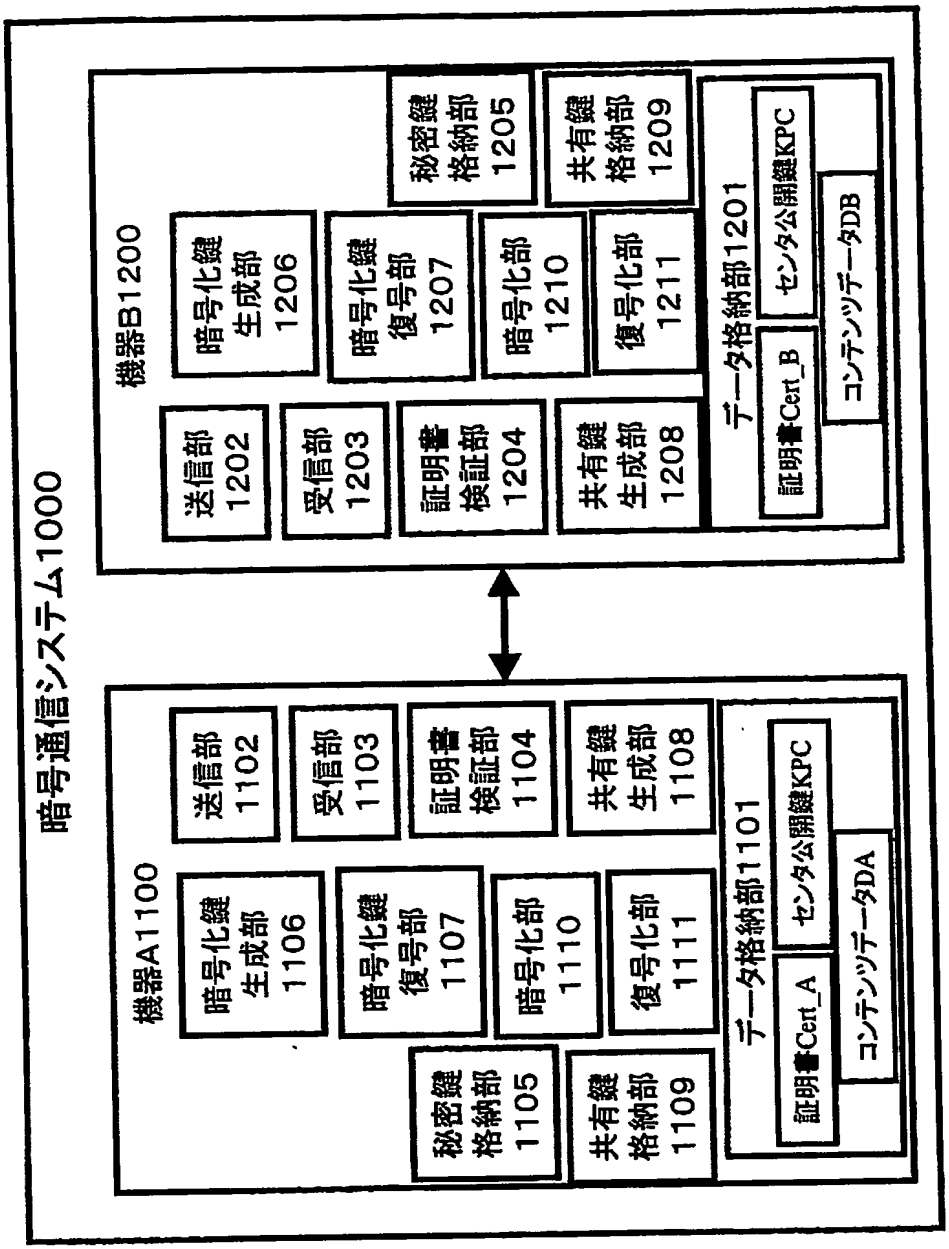
１０００　　暗号通信システム

１１００　　機器Ａ

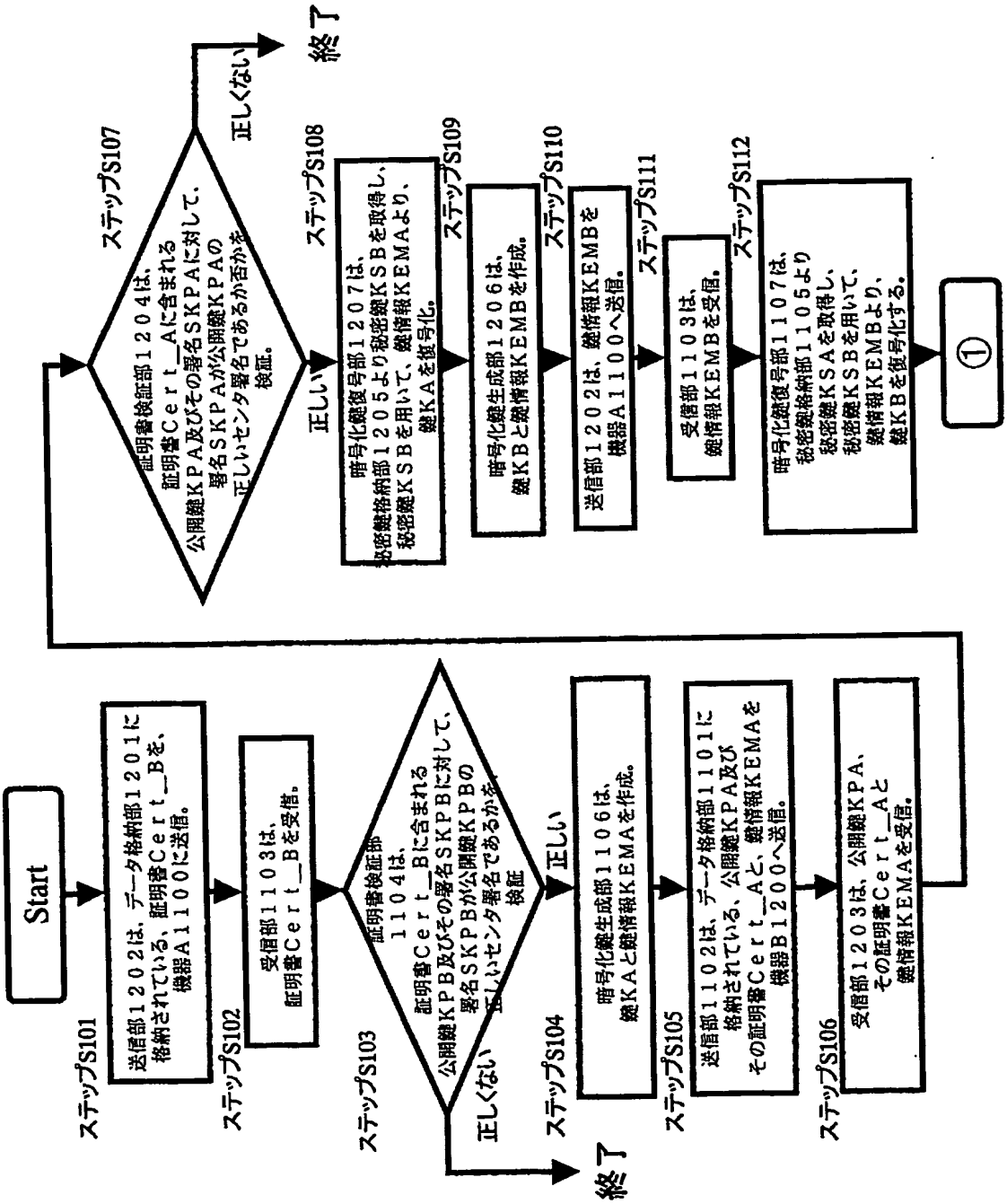
１１０１，１２０１　　データ格納部

１１０２，１２０２　送信部
１１０３，１２０３　受信部
１１０４，１２０４　証明書検証部
１１０５，１２０５　秘密鍵格納部
１１０６，１２０６　暗号化鍵生成部
１１０７，１２０７　暗号化鍵復号部
１１０８，１２０８　共有鍵生成部
１１０９，１２０９　共有鍵格納部
１１１０，１２１０　暗号化部
１１１１，１２１１　復号化部
１２００　機器Ｂ

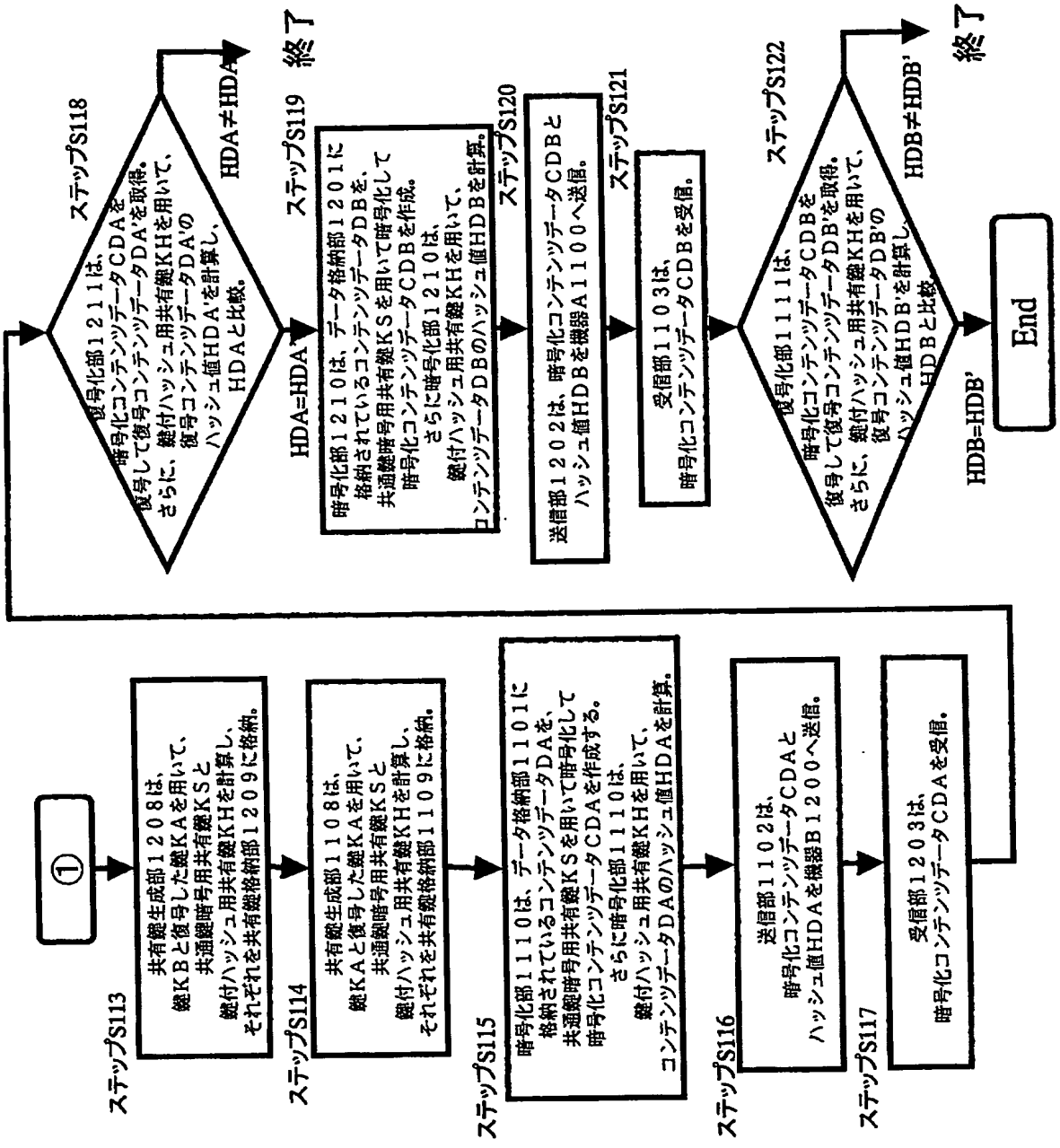
【書類名】図面
【図１】


暗号通信システム1000
機器A1100
暗号化鍵生成部1106
暗号化鍵復号部1107
暗号化部1110
復号化部1111
秘密鍵格納部1105
共有鍵格納部1109
送信部1102
受信部1103
証明書検証部1104
共有鍵生成部1108
データ格納部1101
証明書Cert_A
センタ公開鍵KPC
コンテンツデータDA
機器B1200
暗号化鍵生成部1206
暗号化鍵復号部1207
暗号化部1210
復号化部1211
秘密鍵格納部1205
共有鍵格納部1209
送信部1202
受信部1203
証明書検証部1204
共有鍵生成部1208
データ格納部1201
証明書Cert_B
センタ公開鍵KPC
コンテンツデータDB

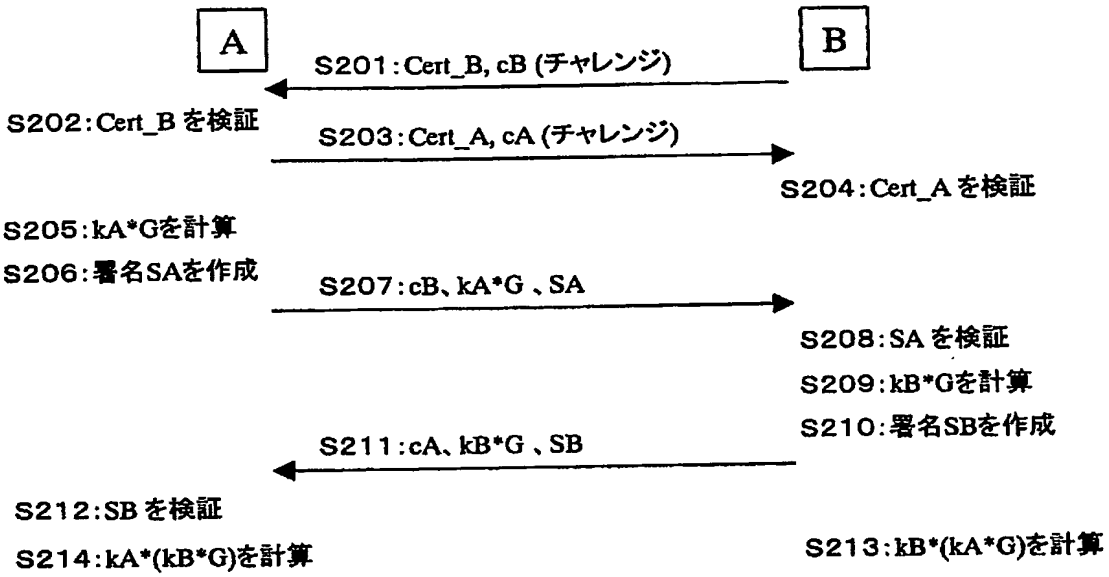
【図２】


Start
ステップS101
送信部１２０２は、データ格納部１２０１に格納されている、証明書Ｃｅｒｔ＿Ｂを、機器Ａ１１００に送信。
ステップS102
受信部１１０３は、証明書Ｃｅｒｔ＿Ｂを受信。
ステップS103
証明書検証部１１０４は、証明書Ｃｅｒｔ＿Ｂに含まれる公開鍵ＫＰＢ及びその署名ＳＫＰＢが公開鍵ＫＰＢの正しいセンタ署名であるかを検証
正しくない
終了
正しい
ステップS104
暗号化鍵生成部１１０６は、鍵ＫＡと鍵情報ＫＥＭＡを作成。
ステップS105
送信部１１０２は、データ格納部１１０１に格納されている、公開鍵ＫＰＡ及びその証明書Ｃｅｒｔ＿Ａと、鍵情報ＫＥＭＡを機器Ｂ１２００へ送信。
ステップS106
受信部１２０３は、公開鍵ＫＰＡ、その証明書Ｃｅｒｔ＿Ａと鍵情報ＫＥＭＡを受信。
ステップS107
証明書検証部１２０４は、証明書Ｃｅｒｔ＿Ａに含まれる公開鍵ＫＰＡ及びその署名ＳＫＰＡが公開鍵ＫＰＡの正しいセンタ署名であるかを検証。
正しくない
終了
正しい
ステップS108
暗号化鍵復号部１２０７は、秘密鍵格納部１２０５より秘密鍵ＫＳＢを取得し、秘密鍵ＫＳＢを用いて、鍵情報ＫＥＭＡより、鍵ＫＡを復号化。
ステップS109
暗号化鍵生成部１２０６は、鍵ＫＢと鍵情報ＫＥＭＢを作成。
ステップS110
送信部１２０２は、鍵情報ＫＥＭＢを機器Ａ１１００へ送信。
ステップS111
受信部１１０３は、鍵情報ＫＥＭＢを受信。
ステップS112
暗号化鍵復号部１１０７は、秘密鍵格納部１１０５より秘密鍵ＫＳＡを取得し、秘密鍵ＫＳＢを用いて、鍵情報ＫＥＭＢより、鍵ＫＢを復号化する。
①

【図３】


①
ステップS113
共有鍵生成部１２０８は、
鍵ＫＢと復号した鍵ＫＡを用いて、
共通鍵暗号用共有鍵ＫＳと
鍵付ハッシュ用共有鍵ＫＨを計算し、
それぞれを共有鍵格納部１２０９に格納。
ステップS114
共有鍵生成部１１０８は、
鍵ＫＡと復号した鍵ＫＡを用いて、
共通鍵暗号用共有鍵ＫＳと
鍵付ハッシュ用共有鍵ＫＨを計算し、
それぞれを共有鍵格納部１１０９に格納。
ステップS115
暗号化部１１１０は、データ格納部１１０１に
格納されているコンテンツデータＤＡを、
共通鍵暗号用共有鍵ＫＳを用いて暗号化して
暗号化コンテンツデータＣＤＡを作成する。
さらに暗号化部１１１０は、
鍵付ハッシュ用共有鍵ＫＨを用いて、
コンテンツデータＤＡのハッシュ値ＨＤＡを計算。
ステップS116
送信部１１０２は、
暗号化コンテンツデータＣＤＡと
ハッシュ値ＨＤＡを機器Ｂ１２００へ送信。
ステップS117
受信部１２０３は、
暗号化コンテンツデータＣＤＡを受信。
ステップS118
復号化部１２１１は、
暗号化コンテンツデータＣＤＡを
復号して復号コンテンツデータＤＡ'を取得。
さらに、鍵付ハッシュ用共有鍵ＫＨを用いて、
復号コンテンツデータＤＡ'の
ハッシュ値ＨＤＡ'を計算し、
ＨＤＡと比較。
HDA≠HDA'
HDA=HDA'
ステップS119
終了
暗号化部１２１０は、データ格納部１２０１に
格納されているコンテンツデータＤＢを、
共通鍵暗号用共有鍵ＫＳを用いて暗号化して
暗号化コンテンツデータＣＤＢを作成。
さらに暗号化部１２１０は、
鍵付ハッシュ用共有鍵ＫＨを用いて、
コンテンツデータＤＢのハッシュ値ＨＤＢを計算。
ステップS120
送信部１２０２は、暗号化コンテンツデータＣＤＢと
ハッシュ値ＨＤＢを機器Ａ１１００へ送信。
ステップS121
受信部１１０３は、
暗号化コンテンツデータＣＤＢを受信。
ステップS122
復号化部１１１１は、
暗号化コンテンツデータＣＤＢを
復号して復号コンテンツデータＤＢ'を取得。
さらに、鍵付ハッシュ用共有鍵ＫＨを用いて、
復号コンテンツデータＤＢ'の
ハッシュ値ＨＤＢ'を計算し、
ＨＤＢと比較
HDB≠HDB'
HDB=HDB'
終了
End

【図４】


A
B
S201:Cert_B, cB (チャレンジ)
S202:Cert_B を検証
S203:Cert_A, cA (チャレンジ)
S204:Cert_A を検証
S205:kA*Gを計算
S206:署名SAを作成
S207:cB、kA*G 、SA
S208:SA を検証
S209:kB*Gを計算
S210:署名SBを作成
S211:cA、kB*G 、SB
S212:SB を検証
S213:kB*(kA*G)を計算
S214:kA*(kB*G)を計算

【書類名】要約書
【要約】
【課題】従来のＩＥＥＥ１３９４の著作権保護規格であるＤＴＣＰの認証鍵共有方法では安全性の証明がなされておらず、安全性に不安が残る。
【解決手段】二者間の通信を以下のように行う。まず、公開鍵証明書認証を相互に行う。次に、鍵カプセル化メカニズムで鍵配送を双方向で行い、２つの共有鍵を得る。さらにその共有鍵の排他的論理和を取ることにより、新たな共有鍵を取得する。その後、新たな共有鍵を共通鍵暗号及び鍵付ハッシュ関数に使用して、二者間でデータ暗号化通信を行う。
【選択図】図１

特願２００３－３５６０７３

出　願　人　履　歴　情　報

識別番号　　[０００００５８２１]

１．変更年月日　　１９９０年　８月２８日
[変更理由]　　新規登録
住　所　　大阪府門真市大字門真１００６番地
氏　名　　松下電器産業株式会社